Attack Surface Management Coverage for Remote Workers with Cortex Xpanse and Cortex XDR

Enable Your IT and SOC Teams to Gain an Attacker's View of Your Remote Employees' Networks

Introduction

Organizations have been forced to accelerate the migration to a remote workforce model despite very limited visibility into the security of their employees' networks. Unfortunately, they have no way of knowing how secure remote worker networks are and whether there are unknown exposures or critical issues open on remote employee devices that are accessible from the public internet.

According to the *2022 Cortex Xpanse Attack Threat Research Report*, Remote Desktop Protocol (RDP) is the most common issue attackers can find on the typical attack surface. One quarter of all issues discovered were related to RDP.[1] RDP could safely be used when employees are in a secure network. However, they become dangerous when exposed to the public internet since they are the attack vector of choice for ransomware attacks.

What about your critical employees, like your VP of Finance working with key financial information or your teams working with critical customer information? Do you know if they are connecting using routers with known vulnerabilities? Do you dynamically alter their access controls using policies based on where they are working, or are they still under the same generous access policies as if they were on your office network? Here are some best practices:

- Ensure that insecure network configurations aren't exposing risky services on corporate devices.
- Gain visibility to dynamically change policies to alter access controls based on employee location.
- Identify endpoints connecting through known vulnerable routers and assess the need to deploy enterprise-grade hardware to key employees.
- Measure the organizational risk associated with key employees working from their home or temporary networks.

Cortex® Xpanse™ is an automated attack surface management (ASM) platform that provides a complete and accurate inventory of an organization's global internet-facing assets and misconfigurations to continuously discover, evaluate, and mitigate security issues on an external attack surface, evaluate supplier risk, or assess the security of acquired companies.

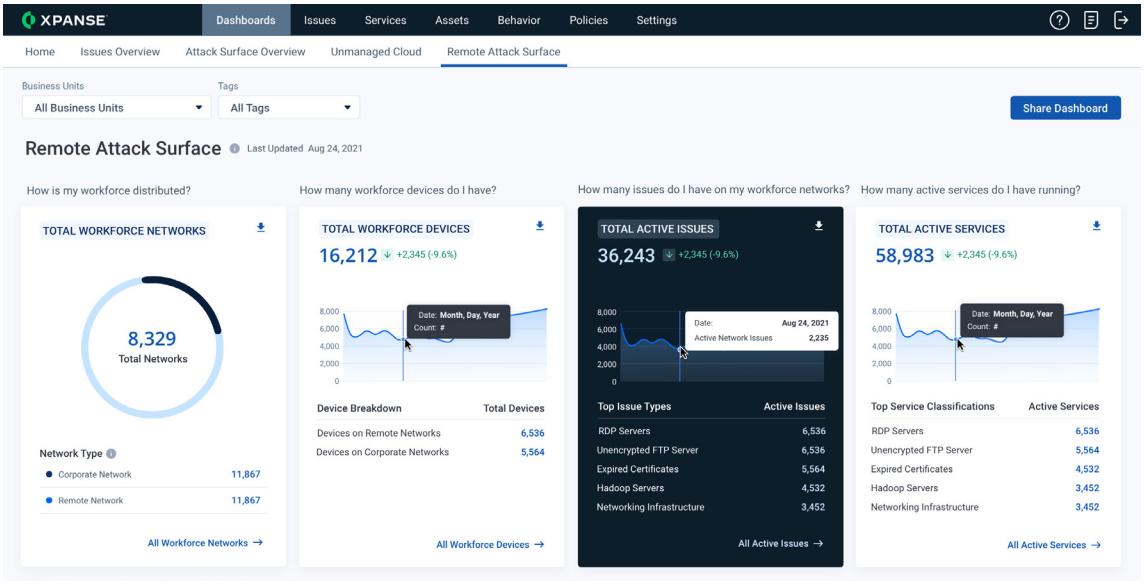

Figure 1: Gain an attacker's point of view of your employees' remote networks

1. *2022 Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks, April 2022, https://www.paloaltonetworks.com/engage/cortex-xpanse-pr/cortex-xpanse-2022-ast.

Secure Your Remote Attack Surface

ASM for Remote Workers is an API integration between Cortex Xpanse and Cortex XDR®. It combines an organization's endpoint details collected by Cortex XDR with public asset information discovered by Xpanse, allowing organizations to effectively identify and alert on security issues on remote worker systems and network environments. The ASM for Remote Workers coverage enables your IT and SOC teams to gain an attacker's view of your remote employee networks. While finding problems is crucial, eliminating them before an exploit occurs is essential to preserving the integrity of a company's security posture.

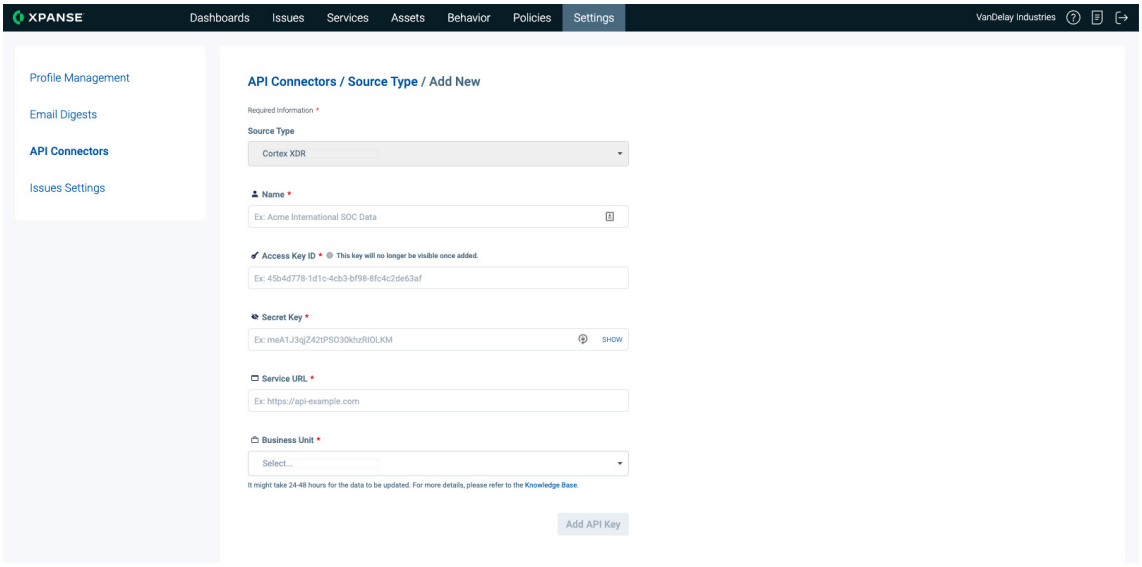

Figure 2: Enter Cortex XDR API Access Key ID and Secret Key to integrate Cortex Xpanse and Cortex XDR

This is where Cortex Xpanse's integration with Cortex XDR is indispensable—and unique in the security industry. By combining Cortex XDR with Xpanse, customers will be able to identify risks and reduce the attack surface related to remote employee environments. Security teams leveraging both technologies will be able to respond to internet-based incidents and secure their remote employees no matter where they work.

Use Cases:

- Identify risks for key remote employees and deploy enterprise-grade hardware selectively.
- Discover the gaps in coverage of Cortex XDR agents in your organization.
- Use visibility to dynamically change policies to alter access controls based on employee location.
- Ensure employees are using VPN service.
- Improve MTTR by providing additional network data to a given incident identified by Cortex XDR.
- Understand co-located employees and employees not using VPNs.
- Find the internal and external IP mapping of your remote workforce.

Combine Cortex XDR's Inside-Out View with Xpanse's Outside-In View

Xpanse can now ingest Cortex XDR endpoint data for assets that have a public IP address and have been seen in the last 24 hours to identify remote workforce devices associated with your organization. All of the networks that Cortex XDR devices are connected to will be visible and categorized as remote or corporate if they overlap with the customer's asset map.

This data will be cross-referenced with Xpanse's global scan data to identify risky issues and services running on the networks where your employees are located, resulting in new Services and Issues in Expander. Cortex XDR gives you internal insight into what's running on those devices, while Xpanse gives you the external perspective and identifies what's exposed to the internet.

With the out-of-the-box integrations of Cortex XSOAR and Cortex XDR, risks discovered by Xpanse can be remediated directly on the device via Cortex XDR, via network configurations, or Xpanse can also send the data to Cortex XSOAR for further automated investigation and remediation.

Cortex Customer Impact

Large Financial Services Firm

An early prototype of this integration provided our customers with visibility into critical vulnerabilities in their remote workers' home networks that they were previously unaware of.

During the beta, Xpanse found the following for the organization:

Table 1: Critical Vulnerabilities in Remote Workers' Home Networks

What Xpanse found	Nearly 60 open RDP servers.	Almost 200 Telnet servers.	More than 1,000 unencrypted logins.
What it is	RDP is a protocol used for communicating with a remote device or server on Windows devices.	Telnet is a protocol used for communicating with a remote device or server.	Login pages that are open to the internet without any encryption.
Why it's bad	RDP is the preferred attack vector for ransomware.	Attackers can install malware or ransomware.	A malicious attacker can easily inject some code into the encrypted login page and steal your info just before it is securely submitted.

About Cortex Xpanse

Cortex Xpanse is a global internet collection and attribution platform that empowers CISOs to continuously discover, evaluate, and mitigate their external attack surface. Today, Xpanse customers collectively represent 12% of the overall IPv4 internet and include leading Fortune 500 companies as well as both US government organizations and military branches.

To learn more about how you can secure your attack surface, visit Cortex Xpanse.

About Cortex XDR

Cortex XDR is the industry's first extended detection and response platform that stops modern attacks by integrating data from any source. Cortex XDR has been designed from the ground up to help organizations like yours secure their digital assets and users while simplifying operations. Using behavioral analytics, it identifies unknown and highly evasive threats targeting your network. Machine learning and AI models uncover threats from any source, including managed and unmanaged devices.

Visit Cortex XDR.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com